

What is claimed is:

1 1. A computer program product for efficiently generating pseudo-random bits, the computer
2 program product embodied on one or more computer readable media and comprising:

3 computer-readable program code means for providing an input value; and

4 computer-readable program code means for generating an output sequence of pseudo-
5 random bits using the provided input value as input to a 1-way function, wherein a length of the
6 input value is substantially shorter than a length of the generated output sequence.

1 2. The computer program product according to Claim 1, wherein the 1-way function is based
2 upon an assumption known as "the discrete logarithm with short exponent" assumption.

3 3. The computer program product according to Claim 1, wherein the 1-way function is
2 modular exponentiation modulo a safe prime number.

1 4. The computer program product according to Claim 3, wherein the input value is used an
2 exponent of the modular exponentiation.

1 5. The computer program product according to Claim 3, wherein a base of the modular
2 exponentiation is a fixed generator value.

1 6. The computer program product according to Claim 4, wherein the length of the input
2 value is 160 bits and a length of the safe prime number is 1024 bits.

1 7. The computer program product according to Claim 1, wherein the length of the input
2 value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

1 8. The computer program product according to Claim 1, further comprising:
2 computer-readable program code means for selecting a subset of bits from the generated
3 output sequence as a next sequential input value, wherein a length of the selected subset is
4 identical to the length of the input value; and

5 computer-readable program code means for generating a next sequential output sequence
6 of pseudo-random bits using the next sequential input value as input to the 1-way function,
7 wherein a length of the next sequential output sequence is identical to the length of the generated
8 output sequence.

9. The computer program product according to Claim 8, further comprising:
2 computer-readable program code means for concatenating bits of the generated next
3 sequential output sequence which are not selected by the computer-readable program code means
4 for selecting to the generated output sequence to form a longer output sequence of pseudo-
5 random bits.

1 10. The computer program product according to Claim 8, wherein the computer-readable
2 program code means for selecting the subset of bits comprises selecting a contiguous group of
3 bits.

1 11. The computer program product according to Claim 8, wherein the computer-readable
2 program code means for selecting the subset of bits comprises selecting a non-contiguous group
3 of bits.

1 12. The computer program product according to Claim 8, further comprising
2 computer-readable program code means for using the longer output sequence as input to an
3 encryption operation.

1 13. A system for efficiently generating pseudo-random bits in a computing environment,
2 comprising:

3 means for providing an input value; and

4 means for generating an output sequence of pseudo-random bits using the provided input
5 value as input to a 1-way function, wherein a length of the input value is substantially shorter than
6 a length of the generated output sequence.

1 14. The system according to Claim 13, wherein the 1-way function is based upon an
2 assumption known as "the discrete logarithm with short exponent" assumption.

1 15. The system according to Claim 13, wherein the 1-way function is modular exponentiation
2 modulo a safe prime number.

1 16. The system according to Claim 15, wherein the input value is used an exponent of the
2 modular exponentiation.

1 17. The system according to Claim 15, wherein a base of the modular exponentiation is a fixed
2 generator value.

1 18. The system according to Claim 16, wherein the length of the input value is 160 bits and a
2 length of the safe prime number is 1024 bits.

1 19. The system according to Claim 13, wherein the length of the input value is at least 160 bits
2 and the length of the generated output sequence is at least 1024 bits.

1 20. The system according to Claim 13, further comprising:
2 means for selecting a subset of bits from the generated output sequence as a next
3 sequential input value, wherein a length of the selected subset is identical to the length of the input
4 value; and

5 means for generating a next sequential output sequence of pseudo-random bits using the
6 next sequential input value as input to the 1-way function, wherein a length of the next sequential
7 output sequence is identical to the length of the generated output sequence.

1 21. The system according to Claim 20, further comprising:

2 means for concatenating bits of the generated next sequential output sequence which are
3 not selected by the means for selecting to the generated output sequence to form a longer output
4 sequence of pseudo-random bits.

1 22. The system according to Claim 20, wherein the means for selecting the subset of bits
2 comprises selecting a contiguous group of bits.

1 23. The system according to Claim 20, wherein the means for selecting the subset of bits
2 comprises selecting a non-contiguous group of bits.

1 24. The system according to Claim 20, further comprising means for using the longer output
2 sequence as input to an encryption operation.

1 25. A method for efficiently generating pseudo-random bits, comprising the steps of:
2 providing an input value; and
3 generating an output sequence of pseudo-random bits using the provided input value as
4 input to a 1-way function, wherein a length of the input value is substantially shorter than a length
5 of the generated output sequence.

1 26. The method according to Claim 25, wherein the 1-way function is based upon an
2 assumption known as "the discrete logarithm with short exponent" assumption.

1 27. The method according to Claim 25, wherein the 1-way function is modular exponentiation
2 modulo a safe prime number.

1 28. The method according to Claim 27, wherein the input value is used an exponent of the
2 modular exponentiation.

1 29. The method according to Claim 27, wherein a base of the modular exponentiation is a
2 fixed generator value.

1 30. The method according to Claim 28, wherein the length of the input value is at least 160
2 bits and a length of the safe prime number is at least 1024 bits.

1 31. The method according to Claim 25, wherein the length of the input value is 160 bits and
2 the length of the generated output sequence is 1024 bits.

1 32. The method according to Claim 25, wherein the length of the input value is at least 160
2 bits and the length of the generated output sequence is at least 1024 bits.

1 33. The method according to Claim 25, further comprising the steps of:
2 selecting a subset of bits from the generated output sequence as a next sequential input
3 value, wherein a length of the selected subset is identical to the length of the input value; and

4 generating a next sequential output sequence of pseudo-random bits using the next
5 sequential input value as input to the 1-way function, wherein a length of the next sequential
6 output sequence is identical to the length of the generated output sequence.

1 34. The method according to Claim 33, further comprising the step of concatenating bits of
2 the generated next sequential output sequence which are not selected by the selecting step to the
3 generated output sequence to form a longer output sequence of pseudo-random bits.

1 35. The method according to Claim 33, wherein the step of selecting the subset of bits
2 comprises selecting a contiguous group of bits.

1 36. The method according to Claim 33, wherein the step of selecting the subset of bits
2 comprises selecting a non-contiguous group of bits.

1 37. The method according to Claim 33, further comprising the step of using the longer output
2 sequence as input to an encryption operation.

1 38. The method according to Claim 25, further comprising the steps of:
2 repeatedly generating additional output sequences, further comprising the steps of:
3 selecting a subset of bits from a next prior generated output sequence as a next
4 input value, wherein a length of the selected subset is identical to the length of the input value;
5 and

generating a next output sequence of pseudo-random bits using the next input value as input to the 1-way function, wherein a length of the next output sequence is identical to the length of the generated output sequence; and
concatenating bits of each of the repeatedly generated additional output sequences which are not selected by the selecting step to form a pseudo-random output sequence.

39. An encryption system, comprising:

means for providing an input value;

means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length of the input value is substantially shorter than a length of the generated output sequence; and

means for using bits of the generated output sequence as input to an encryption operation.

40. The encryption system according to Claim 39, wherein the 1-way function is based upon an assumption known as “the discrete logarithm with short exponent” assumption.

41. The encryption system according to Claim 39, wherein the 1-way function is modular exponentiation modulo a safe prime number.

42. The encryption system according to Claim 41, wherein the input value is used an exponent of the modular exponentiation.

1 43. The encryption system according to Claim 41, wherein a base of the modular
2 exponentiation is a fixed generator value.

1 44. The encryption system according to Claim 42, wherein the length of the input value is 160
2 bits and a length of the safe prime number is 1024 bits.

1 45. The encryption system according to Claim 39, wherein the length of the input value is 160
2 bits and the length of the generated output sequence is 1024 bits.

1 46. The encryption system according to Claim 39, further comprising:
2 means for selecting a subset of bits from the generated output sequence as a next
3 sequential input value, wherein a length of the selected subset is identical to the length of the input
4 value; and

5 means for generating a next sequential output sequence of pseudo-random bits using the
6 next sequential input value as input to the 1-way function, wherein a length of the next sequential
7 output sequence is identical to the length of the generated output sequence.

1 47. The encryption system according to Claim 46, further comprising:
2 means for concatenating bits of the generated next sequential output sequence which are
3 not selected by the means for selecting to the generated output sequence to form a longer output
4 sequence of pseudo-random bits; and

